IN THE SPECIFICATION

Please replace the paragraph beginning on page 1, line 6, with the following amended paragraph:

Authentication of physical objects can be used for many applications, such as conditional access to secure buildings or conditional access to digital data (e.g. stored in a computer or removable storage media), or for identification purposes (e.g. used for charging the identified person for a particular activity). Biometrical authentication is well-known. In such systems, biometrical properties of a human (the physical object) are read using a suitable reader, such as a fingerprint scanner or iris scanner. The properties are compared to reference data. If a match occurs the human is identified or can be granted access. The reference data for the user has been obtained earlier in an ~~enrolment~~ enrollment phase and is stored securely, e.g. in a secure database or smart-card.

Please replace the paragraph beginning on page 2, line 4, with the following amended paragraph:

Typically, the authentication protocols convert the properties cryptographically into a protected control value. The generated

control value is compared to a stored reference control value. The reference data is, for example, stored at a central server at work, in a bank, or in a nightclub where only members have access, or at many other locations where a user has conditional access or needs to be identified. As biometrics are unique identifiers of human beings, privacy problems may arise. People feel uncomfortable with supplying their biometrical information to a large number of seemingly secure databases. Practice has shown that the biometrical information may become available through an insecure implementation (e.g. broken by a hacker) or through misuse by an operator of the system. In particular during the ~~enrolment~~enrollment, the unprotected biometrical data is available. If the information is available at many locations, the chance of misuse increases. It should also be recalled that biometrical data is a good representation of the identity of the user. 'Stealing' some or most of the biometrical data of a person (possibly by breaking only one implementation) can be seen as an electronic equivalent of stealing the person's identity. The stolen data may make it relatively easy to gain access to many other systems protected by biometrical data. Thus, the "identity theft" using the biometric information can have much more serious implications than the "simple" theft of a credit

card. Whereas it is relatively easy to revoke a credit card, it is much more complicated to revoke one's biometrical identity. A further problem of using some biometric information (in particular retina scan) is that it can reveal illness patterns and is therefore very vulnerable to misuse. Some of these problems are also pertinent to authentication of physical objects other than based on biometrical data. For example, a person may have an identity card that can be automatically verified by reading properties of the card. If the card is successful and is used for many applications, revocation of the card becomes cumbersome.

Please replace the paragraph beginning on page 6, line 16, with the following amended paragraph:

Fig. 1 shows a block diagram of the system 100 according to the invention. The system includes an ~~enrolment~~ enrollment device 110 that generates authentication data and stores it in a storage 130. To this end, the ~~enrolment~~ enrollment device includes an input 112 for receiving properties measured from a physical object 105. The properties are measured using a suitable measuring device 120 that may be incorporated into the ~~enrolment~~ enrollment device. The physical object may be a human. Shown is that a fingerprint 105 is

measured from a human. Also other biometrical data may be measured, such as scanning an iris. These techniques are in itself known and will not be described any further. The object may also be non-human. For example, the object may be an electronic identification card. In particular, the object may be a data carrier, such as a carrier of digital audio/video content (e.g. CD). In such a case the object 105 may be combined with the storage 130, i.e. the object also carries the authentication data. If the object is a storage medium object, the properties may be variations in a physical parameter of the storage medium. Those variations may have been made intentionally, specific for each object, or may be random. As long as the variations are sufficiently unique for the object they can be used for the authentication. Irrespective of the physical object, it is assumed that for the physical object a plurality of properties are measured. In principle, the properties are 'analogue', each quantized to a multi-bit value. Typically, at least 8-bit property values will be used. The ~~enrolment~~ enrollment device includes a processor 114 for generating the authentication data. The processor may be any suitable processor, such as for example used in a personal computer. Typically, a general purpose processor is used operated under control of a suitable program. The

program may be stored in a non-volatile memory. Since the ~~enrolment~~ enrollment device creates authentication data that preferably can not easily be broken it is preferred to take some security steps. For example, the ~~enrolment~~ enrollment device may be placed in a secure environment or parts of the processing steps may be executed in a secure module, such as a tamper proof cryptographic module. The authentication data is stored in the storage 130 via output 116.

Please replace the paragraph beginning on page 7, line 8, with the following amended paragraph:

The system further includes at least one authentication device 140. The authentication may in principle be done using the same apparatus as used for the ~~enrolment~~enrollment. In such a case, the ~~enrolment~~enrollment device and authentication device are the same. In the description it will be assumed that both devices are separate to clarify the differences between ~~enrolment~~enrollment and authentication. The ~~enrolment~~enrollment device includes an input 142 for receiving properties measured from the physical object 105. The properties are measured using a suitable measuring device 170 that may be incorporated into the authentication device.

Preferably, the measurement devices 120 and 170 are of a similar design. The same physical object is measured as for which the authentication data has been created by the authentication device 110. The authentication device includes a processor 144 for comparing the object properties against the authentication data. The processor may be any suitable processor, such as for example used in a personal computer. Typically, a general purpose processor is used operated under control of a suitable program. The program may be stored in a non-volatile memory. The input of the authentication device is also used for receiving the authentication data from the storage 130. It will be appreciated that the ~~enrolment~~enrollment device, storage, and authentication device may be physically far removed. If so, suitable communication means may be used for exchanging the authentication data. The storage 130 may also be incorporated into the ~~enrolment~~enrollment device.

Please replace the paragraph beginning on page 9, line 10, with the following amended paragraph:

~~Enrolment~~Enrollment performed by the ~~enrolment~~enrollment device:

During this phase the person or physical object has to visit the ~~enrolment~~enrollment device, e.g. located at a Certification

Authority (CA). The properties of the object/person are measured, processed and stored as reference data V for later use together with any helper data W that may have been used to steer the processing. Preferably, the helper data is determined by the properties of X. In an on-line application, these data can be stored in a central database or these data can be certified by a digital signature of the CA and be given to the service provider.

Please replace the paragraph beginning on page 9, line 18, with the following amended paragraph:

In short, the ~~enrolment~~enrollment device according the invention performs the following steps:

(1) Get measurements, giving a property set Y

(2) Create robust properties from the property set Y, giving a set of robust properties I

(3) Reduce the information in property set I, giving a property set A

(4) Generate a control value V based on property set A

(5) Store V and any helper data W that may have been used to steer the processing

As will be described below, steps 2 and 3 can be seen as a

signal processing function G operating on the property set Y, under control of the helper data W, giving as output G(Y,W). This forms the property set A. The signal processing may show steps 2 and 3 as separate sequential processing steps (illustrated below in two embodiments) but can also be performed in one integrated processing step (shown below for one embodiment). The helper data W may steer both steps 2 and 3. For authentication, typically steps 2 and 3 can be performed in one operation, since W is already known.

Please replace the paragraph beginning on page 9, line 32, with the following amended paragraph:

The control value V may simply be the property set A. In order to protect the communication line between the ~~enrolment~~enrollment device, storage, and authentication device, in a preferred embodiment, creating the control value V includes performing a cryptographic function on properties of the property set A. Preferably, the cryptographic function is a homomorphic one-way function. A suitable hash is the function. $r \mapsto r^2 \bmod n, m \mapsto g^{m+nr} \bmod n^2$ for a randomly chosen $r \in Z_n$ and g being the generator of a subgroup (Paillier encryption function). The encrypted secret derived from the biometric measurements are then stored at the database. These

homomorphic one-way functions allow to set-up a Zero-Knowledge protocol for checking the knowledge of the template without revealing any information. As the communication during Zero-Knowledge protocols preferably changes every session, the communication line is better protected.

Please replace the paragraph beginning on page 10, line 23, with the following amended paragraph:

Note: the helper data (if any) is used in an analogous way to steer the processing as done during the ~~enrolment~~enrollment. For authentication, typically steps 2 and 3 can be performed in one operation, since it is already known from the ~~enrolment~~enrollment which properties are robust (described by helper data W), so in many embodiments it will be possible to perform step 4 on only selected properties without explicitly creating the smaller set.

Please replace the paragraph beginning on page 11, line 11, with the following amended paragraph:

As will be described below, the signal processing of two preferred embodiment is based on statistical properties of the signal X and/or noise E. These statistical properties may be

estimated in any suitable way, for example by taking the measurements a number of times during the ~~enrolment~~enrollment and then estimate the statistical properties using a suitable statistical estimation well-known to persons skilled in the art.

Please replace the paragraph beginning on page 11, line 28, with the following amended paragraph:

For the robust properties of set I_1 are selected those properties of Y with sufficiently large absolute values. Sufficiently large means that the contribution of X_i to Y_i is expected to be larger than the contribution of E_i, so a signal to noise (S/N) ratio of at least 1. By performing several measurements during the ~~enrolment~~enrollment a good statistical estimation of the noise values E_i can be obtained. Preferably, only properties of Y_i that clearly exceed this estimate (e.g. $S/N > 3$) are used as being robust, i.e. assigned to set I_1. If the noise level of the measurement procedure is known it is not required to perform several measurements to obtain such an estimate.

Please replace the paragraph beginning on page 16, line 22, with the following amended paragraph:

Additionally or alternatively, the information can be reduced by only selecting a subset of the property set I_1. The selection that is made during the ~~enrolment~~enrollment can be described by helper data W. This helper data is then stored as part of the authentication data and used during authentication to achieve the selection of the same subset at that moment. Preferably, for different applications different, unique helper data W is created. In this way each application uses its own subset (that may of course overlap).

Please replace the paragraph beginning on page 18, line 9, with the following amended paragraph:

In the first described embodiment, W can be chosen to a random matrix. Suppose that the measurements X are n-dimensional real vectors. During the ~~enrolment~~enrollment phase, choose a random and orthonormal matrix$W$. Let =WY, now select components of with sufficiently large absolute values. In principle, one should expect a large number of such coordinates. Using some (but not all!) of

these coordinates, generate the secret $C=(c_1,...,c_k)$, where $c_k=H(\alpha_{i_k})$. In other words, $C=H(\tilde{W}Y)$, where $\tilde{W}$ is a $k\times n$ matrix, obtained from W by selecting rows $i_1,...i_k$. If W does not lead to a sufficient number of large components, another random matrix may be generated.

Please replace the paragraph beginning on page 18, line 19, with the following amended paragraph:

~~Enrolment~~Enrollment, as illustrated in Fig. 2A

(1) Get measurements $Y=(Y_1,...,Y_n)\in R^n$ of certain actual corresponding properties (such as biometrics) $X=(X_1,...,X_n)$ of the object;

(2) Create robust properties from the property set Y, giving a set of robust properties I_1

- Perform transformation = Y , where Γ sorts the vector components according to an estimated signal to noise ratio~~.~~;
- Select set I: I_1=I ( ) ={| $_i$| > }, where δ is derived from a noise level in the measurements;

(3) Reduce the information:

- Select subset of I_1; selection defines selection function W(X) that is a subset of the transformation , thus the subset of selected robust properties is formed by:

  $\alpha_{i_j} = WY$;

- Generate secret by performing contraction on the subset:

  e.g. $c_j = H(\alpha_{i_j})$ (where H is the Heaviside function) giving a binary code word C of length

  k n;

(4) Generate control value V, e.g. by using a collision resistant one-way hash function h V= h(C);

(5) Store: W, V.